Power Integral Bases in Orders of Composite Fields

István Gaál, Péter Olajos and Michael Pohst

CONTENTS

We consider the existence of power integral bases in composites of polynomial orders of number fields. We prove that if the degree of the composite field equals the product of the degrees of its subfields and the minimal polynomials of the generating elements of the polynomial orders have a multiple linear factor in their factorization modulo q, then the composite order admits no power integral bases. As an application we provide several examples including a parametric family of "simplest sextic fields."

1. INTRODUCTION

For any primitive element $\alpha \in \mathbb{Z}_K$ the *index of* α is defined as the module index

$$I(\alpha) := (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha]).$$

Obviously, the discriminant and index of α satisfy

$$D_{K/\mathbb{Q}}(\alpha) = I(\alpha)^2 D_K,$$

where D_K is the discriminant of the field K. The element α generates a *power integral basis* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in K if and only if $I(\alpha) = 1$.

The problem of existence and construction of power integral bases in algebraic number fields has been intensively studied in recent years; for a survey we refer to [Gaál 99].

2. COMPOSITE FIELDS

Let $f, g \in \mathbb{Z}[x]$ be distinct monic irreducible polynomials (over $\mathbb{Q}$) of degrees m and n, respectively. Let φ be a root of f and let ψ be a root of g. Set $L = \mathbb{Q}(\varphi)$, $M = \mathbb{Q}(\psi)$ and assume that the composite field $K = LM$ has degree mn. We also assume that there is a prime number q, such that both f and g have a multiple linear factor (at least square) mod q, that is, there exist a_f and a_g in $\mathbb{Z}$ such that

$$\begin{aligned} f(a_f) \equiv f'(a_f) \equiv 0 \pmod{q}, \\ g(a_g) \equiv g'(a_g) \equiv 0 \pmod{q}. \end{aligned} \tag{2–1}$$

2000 AMS Subject Classification: Primary 11D57; Secondary 11R04
Keywords: Composite fields, power integral bases

1058-6458/2001 $0.50 per page

Remark 2.1. Our assumption implies that q divides both the discriminant $d(f)$ of the polynomial f and the discriminant $d(g)$ of g.

Remark 2.2. In [Gaál 98] we considered fields that are composites of subfields with coprime discriminants. According to the remark above in our case the fields we consider are composites of subfields whose discriminants are not coprime. This is the case in many interesting examples some of which we list at the end of the paper.

Consider the order $\mathcal{O}_f = \mathbb{Z}[\varphi]$ of the field L, the order $\mathcal{O}_g = \mathbb{Z}[\psi]$ of the field M and the composite order $\mathcal{O}_{fg} = \mathcal{O}_f\mathcal{O}_g = \mathbb{Z}[\varphi,\psi]$ in the composite field $K = ML$. Note that $\{1,\varphi,\dots,\varphi^{m-1}\}$, $\{1,\psi,\dots,\psi^{n-1}\}$ and

$$\{1,\varphi,\dots,\varphi^{m-1},\psi,\varphi\psi,\dots,\varphi^{m-1}\psi,\\ \dots,\psi^{n-1},\varphi\psi^{n-1},\dots,\varphi^{m-1}\psi^{n-1}\},$$

are $\mathbb{Z}$-bases of $\mathcal{O}_f$, $\mathcal{O}_g$ and $\mathcal{O}_{fg}$, respectively.

Our main result is the following:

Proposition 2.3. *Under the assumptions above the index of any primitive element of the order $\mathcal{O}_{fg}$ is divisible by q.*

As a consequence we have:

Proposition 2.4. *Under the assumptions above the order $\mathcal{O}_{fg}$ has no power integral bases.*

At the end of the paper we give several applications of the propositions.

Note that a similar phenomenon occurs for composite fields in other cases as well, cf. [Gaál 95], [Gaál 98], [Gaál 00].

3. PROOF OF PROPOSITION 1

Denote the conjugates of $\varphi \in L$ by $\varphi^{(i)}$ $(1 \le i \le m)$ and the conjugates of $\psi \in M$ by $\psi^{(j)}$ $(1 \le j \le n)$. Denote by $\gamma^{(i,j)}$ the conjugate of any element $\gamma \in K$ under the automorphism mapping φ to $\varphi^{(i)}$ and ψ to $\psi^{(j)}$ $(1 \le i \le m, 1 \le j \le n)$.

The discriminants of the polynomials f and g are

$$d(f) = \prod_{1\le i<j\le m} (\varphi^{(i)} - \varphi^{(j)})^2$$
$$d(g) = \prod_{1\le i<j\le n} (\psi^{(i)} - \psi^{(j)})^2. \tag{3–1}$$

These are also the discriminants of the bases $\{1,\varphi,\dots,\varphi^{m-1}\}$ of the order $\mathcal{O}_f$ and $\{1,\psi,\dots,\psi^{n-1}\}$ of the order $\mathcal{O}_g$, respectively. The discriminant of the order $\mathcal{O}_{fg}$ is

$$D(\mathcal{O}_{fg}) = d(f)^n \cdot d(g)^m. \tag{3–2}$$

We can represent any element $\alpha \in \mathcal{O}_{fg}$ in the form

$$\alpha = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} x_{ij}\varphi^i\psi^j \tag{3–3}$$

with $x_{ij} \in \mathbb{Z}$. The index of α (generating K over $\mathbb{Q}$) corresponding to the order $\mathcal{O}_{fg}$ is defined to be the $\mathbb{Z}$-module index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_{fg}$. It is

$$I_{\mathcal{O}_{fg}}(\alpha) = \frac{1}{\sqrt{|D(\mathcal{O}_{fg})|}} \prod_{(i_1,j_1)<(i_2,j_2)} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|$$

where the pairs of indices are ordered lexicographically. Now we rearrange the factors in the product above. Using (3–1) and (3–2) we have

$$\begin{aligned} I_{\mathcal{O}_{fg}}(\alpha) \quad = \quad & \prod_{i=1}^{m}\prod_{1\le j_1<j_2\le n} \left|\frac{\alpha^{(i,j_1)} - \alpha^{(i,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}}\right| \\ & \times \prod_{j=1}^{n}\prod_{1\le i_1<i_2\le m} \left|\frac{\alpha^{(i_1,j)} - \alpha^{(i_2,j)}}{\varphi^{(i_1)} - \varphi^{(i_2)}}\right| \\ & \times \prod_{\substack{(i_1,j_1)<(i_2,j_2)\\ i_1\ne i_2\\ j_1\ne j_2}} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|. \end{aligned} \tag{3–4}$$

Obviously, the factors that appear in (3–4) are algebraic integers.

For any $1 \le i_1 < i_2 \le m$ and $1 \le j_1 < j_2 \le n$ we have

$$\left(\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}\right) + \left(\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}\right) + \left(\alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}\right) = 0$$

which implies the equation

$$\left(\varphi^{(i_1)} - \varphi^{(i_2)}\right)\varepsilon + \left(\psi^{(j_1)} - \psi^{(j_2)}\right)\eta + \rho = 0 \tag{3–5}$$

with

$$\varepsilon = \frac{\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}}{\varphi^{(i_1)} - \varphi^{(i_2)}},$$
$$\eta = \frac{\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}},$$
$$\rho = \alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}.$$

Since these elements are factors in (3–4) they are algebraic integers lying in the $\mathbb{Z}$-order $\mathcal{O} = \mathcal{O}_{i_1,i_2,j_1,j_2} = \mathbb{Z}[\varphi^{(i_1)},\varphi^{(i_2)},\psi^{(j_1)},\psi^{(j_2)}]$.

Let us fix those indices $1 \le i_1 < i_2 \le m$ and $1 \le j_1 < j_2 \le n$ for which $\varphi^{(i_1)} \equiv \varphi^{(i_2)} \pmod{q}$ and also $\psi^{(j_1)} \equiv \psi^{(j_2)} \pmod{q}$. Consider equation (3–5) modulo q.

By our assumptions $\varphi^{(i_1)} - \varphi^{(i_2)} \equiv 0 \pmod{q}$ and $\psi^{(j_1)} - \psi^{(j_2)} \equiv 0 \pmod{q}$, hence by equation (3–5) we get $\rho = \alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)} \equiv 0 \pmod{q}$. This is one of the algebraic integer factors of $I(\alpha)$, hence $q|I(\alpha)$.

4. APPLICATIONS

4.1 A Cyclic Sextic Field

Consider the sextic field K generated by a root of $h(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$. This is a totally real cyclic sextic field with discriminant $D_K = 453789 = 3^3 7^5$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant 49) where φ is a root of $f(x) = x^3 + 4x^2 + 3x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x+6)^3 \pmod{7}$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{21})$. The polynomial $g(x) = x^2 - x - 5$ has $\psi = (1 + \sqrt{21})/2$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv (x - 1/2)^2 \pmod{7}$. Proposition 1 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 7, hence it has no power integral basis.

4.2 A Non-Cyclic Sextic Field

Consider the sextic field K generated by a root of $h(x) = x^6 - 12190x^4 + 256565x^2 - 12167$. This is a totally real sextic field with Galois group D_6, discriminant $D_K = 2^6 17^2 23^3 647^2$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant $252977 = 17 \cdot 23 \cdot 647$ and Galois group S_3) where φ is a root of $f(x) = x^3 - 22x^2 - 23x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x+15)(x+16)^2 \pmod{23}$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{23})$. The polynomial $g(x) = x^2 - 23$ has $\psi = \sqrt{23}$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv x^2 \pmod{23}$. Proposition 1 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 23, hence it has no power integral basis.

4.3 The Parametric Family of Simplest Sextic Fields

Assume $3 \nmid t$, $t \neq -8, \pm 5$. Let us consider the family of sextic fields K_t generated by a root β of the polynomial

$$h_t(x) = x^6 - 2tx^5 - (5t+15)x^4 - 20x^3 + 5tx^2 + (2t+6)x + 1.$$

This family of fields is called the "simplest sextic fields". It has some attractive properties which are listed in [Lettl et al. 98]. These fields are totally real cyclic fields. Let p be a prime dividing $q = t^2 + 3t + 9$. We have $d(h_t) = 6^6 q^5$. Note that $h_t(x) \equiv (x - t/3)^6 \pmod{p}$ (the "simplest quintic fields" have a similar property, cf. [Gaál and Pohst 97]).

The cubic subfield L_t of K_t is generated by a root φ of $f_t = x^3 - tx^2 - (t+3)x - 1$ with $d(f_t) = q^2$. These are the "simplest cubic fields", totally real, cyclic. It is well known that $\{1, \varphi, \varphi^2\}$ is an integral basis of $\mathbb{Z}[\varphi]$. Note that $f_t(x) \equiv (x - t/3)^3 \pmod{p}$.

The quadratic subfield of K_t is $M_t = \mathbb{Q}(\sqrt{q})$.
If $q \equiv 2, 3 \pmod{4}$ then set $g_t(x) = x^2 - q$ with $d(g_t) = 4q$ and with a root $\psi = \sqrt{q}$. In this case $g_t(x) \equiv x^2 \pmod{p}$.
If $q \equiv 1 \pmod{4}$ then set $g_t(x) = x^2 - x - (q-1)/4$ with $d(g_t) = q$ and with a root $\psi = (1 + \sqrt{q})/2$. In this case $g_t(x) \equiv (x - 1/2)^2 \pmod{p}$.
In both cases $\{1, \psi\}$ is an integral basis of M_t.

Consider now the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$. By Proposition 1 the indices of the primitive elements of $\mathcal{O}_{fg}$ are all divisible by p, hence $\mathcal{O}_{fg}$ has no power integral bases.

4.4 A Field of Higher Degree

This is an example to illustrate that our results are easily applicable also to suitable fields of higher degrees.

Let φ be a root of $f(x) = x^5 - 2x^4 + 7x^2 + 6x + 5$. The quintic field $L = \mathbb{Q}(\varphi)$ has no non-trivial subfields. Let ψ be a root of $g(x) = x^8 + 13x^7 + 55x^6 + 75x^5 + 2x^3 - x^2 - 143x - 525$. The octic field $M = \mathbb{Q}(\psi)$ has no non-trivial subfields, either. We have

$$\begin{aligned} f(x) &\equiv (x+16)^2(x^3 + 16x + 5) \pmod{17} \\ g(x) &\equiv (x+5)^2(x^3 + 12x^2 + 2x + 14) \\ &\quad \times (x^3 + 8x^2 + 4x + 7) \pmod{17} \end{aligned}$$

hence our Proposition 1 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 40. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Proposition 1 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 17, hence $\mathcal{O}_{fg}$ admits no power integral bases.

ACKNOWLEDGEMENTS

The research of István Gaál was supported in part by Grants T 29330 and T 037367 from the Hungarian National Foundation for Scientific Research and by FKFP 0343/2000. The research of Péter Olajos was supported by FKFP 0343/2000.

REFERENCES

[Gaál 95] I.Gaál. "Computing elements of given index in totally complex cyclic sextic fields." *J. Symbolic Computation* **20** (1995), 61–69.

[Gaál 98] I.Gaál. "Power integral bases in composits of number fields." *Canad. Math. Bulletin* **41** (1998), 158–165.

[Gaál 99] I.Gaál. "Power integral bases in algebraic number fields." *Annales Univ. Sci. Budapest., Sect. Comp.* **18** (1999), 61–87.

[Gaál 00] I.Gaál. "Solving index form equations in fields of degree nine with cubic subfields." *J. Symbolic Comput.* **30** (2000), 181–193.

[Gaál and Pohst 97] I.Gaál and M.Pohst. "Power integral bases in a parametric family of totally real quintics." *Math. Comp.* **66** (1997), 1689–1696.

[Lettl et al. 98] G.Lettl, A.Pethő, P.Voutier. "On the arithmetic of simplest sextic fields and related Thue equations." In *Number Theory*, eds. K.Győry, A.Pethő, V.T.Sós, pp. 331–348, Walter de Gruyter, Berlin-New York, 1998.

István Gaál, University of Debrecen, Mathematical Institute H-4010 Debrecen Pf.12., Hungary (igaal@math.klte.hu)

Péter Olajos, University of Debrecen, Mathematical Institute H-4010 Debrecen Pf.12., Hungary (olaj@math.klte.hu)

Michael Pohst, Technische Universität Berlin, Fakultät II, Institut für Mathematik, Strasse des 17. Juni 136, Berlin 10623, Germany (pohst@math.tu-berlin.de)

Received February 28, 2001; accepted in revised form August 14, 2001.